|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Student Name | |  | Student Number |  | |
| Unit Code/s & Name/s | | VU23220 Develop and carry out a cyber-security industry project  VU23221 Evaluate and test an incident response plan for an enterprise | | | |
| Cluster Name  *If applicable* | | Incident Response Project | | | |
| Assessment Type | | Case Study  Assignment  Project  Other *(specify)* | | | |
| Assessment Name | | Incident Response Project Planning Report | Assessment Task No. | | 1 of 2 |
| Assessment Due Date | | Week 8 | Date Submitted | / / | |
| Assessor Name | |  | | | |
| **Student Declaration:** I declare that this assessment is my own work. Any ideas and comments made by other people have been acknowledged as references. I understand that if this statement is found to be false, it will be regarded as misconduct and will be subject to disciplinary action as outlined in the TAFE Queensland Student Rules. I understand that by emailing or submitting this assessment electronically, I agree to this Declaration in lieu of a written signature. | | | | | |
| Student Signature |  | | Date | / / | |
| **PRIVACY STATEMENT:** TAFE Queensland is collecting your personal information on this form for the purpose of assessment. In accordance with the Information Privacy Act 2009 (Qld), your personal information will only be accessed by staff employed by TAFE Queensland for the purposes of conducting assessment. Your information will not be provided to any other person or agency unless you have provided TAFE Queensland with permission, if authorised under our Privacy Policy (available at <https://tafeqld.edu.au/global/privacy-policy.html>) or disclosure is otherwise permitted or required by law. Your information will be stored securely. If you wish to access or correct any of your information, discuss how it has been managed or have a concern or complaint about the way the information has been collected, used, stored, or disclosed, please contact the TAFE Queensland Privacy Officer at [privacy@tafeqld.edu.au](mailto:privacy@tafeqld.edu.au) | | | | | |

|  |  |
| --- | --- |
| Instructions to Student | **General Instructions:**  MidTown IT has assigned you to plan and oversee the implementation of an Incident Response Team Exercise (IRTx) for RightPoint. The task involves preparing an Incident Response Plan, establishing red, blue and purple teams, assigning tasks and responsibilities to team members, and assigning resources to the project.  Your teacher/assessor will take on the role of the Project Sponsor assigned to this project by MidTown IT and the RightPoint CSO. Read the project documentation provided and familiarise yourself with the Project Scenario or Case Study before proceeding with portfolio tasks. Confirm anything you need clarification about the project with your manager (teacher/assessor). You must clearly understand the scenario and tasks you need to complete.  In this assessment you are required to complete a project portfolio that is divided into three (3) parts:   * PART 1 – Determining Project Context * PART 2 – Establishing Project Team * PART 3 – Communication Strategy and Reporting Hierarchy * PART 4 – Evaluate Current IRP * PART 5 – Develop IRP * PART 6 – Stakeholder Status Reporting   **Storage Devices:**   * You are required to provide your own storage devices.   **Materials Required:**   * Access to the Internet * Access to Connect (LMS) * Access to a virtual networking environment * Access to a virtual testing environment * Access to Word processing software, such as Microsoft Word * Access to special-purpose tools, equipment and materials to complete the assessment.   **For Online Delivery:**   * You are to supply their own PC or laptop and peripherals and internet access * You will require permission to install the required software * You will require access to Microsoft Office or a similar application   **Documents provided:**   * RightPoint Scenario or Case Study * RidhtPoint Project Charter template * RightPoint Current IRP * Communications Plan template   **Assessment Criteria:**  To achieve a satisfactory result, your assessor will look for your ability to demonstrate the following key skills/tasks/knowledge to an acceptable industry standard. Demonstrated ability to:   * Determine project context, scope, objectives and expected outcomes * Schedule project tasks, timeframes and costs * Identify the resources and support needed to implement the incident response plan * Determine process to manage risk or unexpected events and their impact on the project * Determine resources and support needed to implement the project * Determine functions and operations of selected resources * Assign responsibilities to team members * Evaluate the suitability of resources and support strategies * Evaluate / Design an Incident Response Plan * Establish red, blue and purple teams * Determine and measure the performance criteria of the project team * Create an implementation plan that ensures minimum disruptions * Evaluate existing risk strategies * Determine the training needs of users to implement the project   Refer to the marking criteria for specific details:  VU23220\_VU23221\_AT1\_MC\_TQM\_V1  **Details of location:**  TAFE will provide a simulated work environment in the classroom. Research activities may be conducted in the classroom or at home.  If you are unable to attend a scheduled assessment activity, you must notify your teacher before the assessment is due and supply a doctor's certificate and approval from the team manager for an extension.  **Time restrictions:**  This assignment is designed to take place over 8 weeks or approximately 32 hours. The student is expected to attend classes as per timetable details and should be able to commit up to 3 hours per week of their own time to study or study related activities.  **Interactions:**  Teamwork skills are essential in the IT industry therefore you should work in teams to consult and collaborate on practical activities. However, each student must complete the assessment tasks individually (unless indicated).  **Level of assistance permitted:**  Staff cannot directly show students answers or solutions but support and guide them to complete tasks individually. Teachers and tutors should be available in class, and accessible by email for students working from home.  **Reasonable Adjustments:**  Reasonable adjustments are available to students for a variety of reasons, including: disability, language, literacy and numeracy (LLN) problems or extenuating circumstances. Talk to your teacher, counsellor or disability officer if you require extra support or an extension based on the conditions identified.  **Number of Attempts:**  You will receive up to two (2) attempts at this assessment task. Should your 1st attempt be unsatisfactory (U), your teacher will provide feedback and discuss the relevant sections / questions with you and will arrange a due date for the submission of your 2nd attempt. If your 2nd submission is unsatisfactory (U), or you fail to submit a 2nd attempt, you will receive an overall unsatisfactory result for this assessment task. Only one re-assessment attempt may be granted for each assessment task.  ***For more information, refer to the Student Rules.***  **Work, Health and Safety:**  The work environment should be assessed for safety prior to class. Special consideration should be taken regarding potential ICT related hazards such as tripping hazards, electromagnetic radiation, ergonomics, and posture. TAFE Queensland health and safety policies and procedures should be followed at all times. |
| Submission Details | **Evidence Required to be Submitted:**  Insert your details on the cover page and sign the Student Declaration. Include this template with your submission.  **Submission via Connect:**  Upload a single file into Assessment 1 (AT1) Assignment Folder in Connect.  Multiple files can be compressed into a single file.  Name the file:  VU23220\_VU23221\_AT1\_Surname\_Student Number  TAFE Queensland Learning Management System (Connect)  **Accessing Connect:**  Connect URL: https://connect.tafeqld.edu.au/d2l/login  Username: 9-digit student number  Password: <your password>  For password reset go to: <https://passwordreset.tafeqld.edu.au/default.aspx> |
| Instructions for the Assessor | **Specifications of assessment:**  To achieve a satisfactory result in this assessment, students must successfully complete ALL tasks identified in the Marking Guide.  Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the cyber security field of work and include access to:   * project requirements   Ensure that students read and familiarise themselves with the Project Scenario provided and relevant files and/or resources before attempting the assessment.  **Level of Assistance Permitted:**  Teachers and tutors should be available in class, and accessible by email for students working from home. Staff cannot directly show students answers but support and guide them to complete tasks individually. Students with disability will receive reasonable adjustments.  **Interactions:**  Teamwork skills are essential in the IT industry therefore you should work in teams to consult and collaborate on practical activities. However, each student must complete the assessment tasks individually (unless indicated).  **Contingencies:**  Reasonable adjustment is available to students for a variety of reasons, including: disability, language, literacy and numeracy (LLN) problems or extenuating circumstances.  **Work, Health and Safety:**  The work environment should be assessed for safety prior to class. Special consideration should be taken regarding potential ICT related hazards such as tripping hazards, electromagnetic radiation, ergonomics, and posture. TAFE Queensland health and safety policies and procedures should be followed at all times. |
| Note to Student | An overview of all Assessment Tasks relevant to this unit is located in the Unit Study Guide.  If you have any question or need help regarding this assessment item please contact your teacher/tutor through email or during face-to-face sessions. |

# PART 1 Determining Project Context

* 1. 1.1 Analyse the project scenario presented and write down any questions you have about the project. Clarify with your assessor any doubts you have expressed in your questions. Submit the questions with your assessment.

1.2 Using the template provided, prepare a Project Charter/Project Brief for the Incident Response Project (IRP). The document shall not exceed ten (10) pages and shall include the following information:

1. Project purpose
2. Project scope and boundaries
3. Project objectives and expected outcomes (at least three (3) project deliverables)
4. Project methodology or approach
5. Details of key project milestones
6. Deliverables at least three (3) deliverables)
7. Timeline for completion of the project
8. A detailed work breakdown structure listing all required tasks
9. A summary of costs
10. A Gantt Chart
11. A statement outlining the major implications or business impact that cyber incidents have or could have on the organisation

# PART 2 Establishing Project Team

In this task, you must hold/attend a meeting to select team members for the Incident Response Team Exercise (IRTx) and assign roles, responsibilities, and activities within your team. You must also decide how the team’s performance will be measured. Management established the following guidelines for the exercise:

* Teams (Red\Blue) should consist of between four (2) and six (3) members
* There will be two student teams red and blue per group
  + Observer (purple) team will be the instructor
* Roles and responsibilities must be outlined for each member
* Your assessor will on the role of Project Sponsor / Manager
* Roles should include Quality Assurance Lead and Communications Lead
* A minimum of three (3) performance metrics must be used to evaluate team performance

2.1 Prepare a briefing report outlining:

1. Composition of the teams
2. Roles and responsibilities of members
3. Fundamental red, blue and purple team activities
4. Performance metrics

The briefing must also comply with the management guidelines listed earlier.

2.2 Submit the briefing report together with the minutes of the meeting in accordance with the Communication Strategy and Reporting Guidelines (PART 3)

# PART 3 Communication Strategy and Reporting Hierarchy

3.1 Using the template provided, prepare a communication plan for the Incident Response Project. The communication plan must address the following:

1. Purpose
2. Scope
3. Goals and Objectives
4. Communication roles
5. Communication tools and methods
6. Scheduling of meetings
   * Who will chair the meeting?
   * Who will take the minutes?
7. Frequency of meetings
8. Meetings reporting – Minutes and Agendas
9. Structure of meetings
   * Concept development meeting
   * Initial planning meeting
   * Mid-point planning meeting
   * Final planning meeting status reporting to project sponsor
     + Weekly meetings with the teacher
     + Final presentation outline
10. Plan Updates and Approval Record

# PART 4 Re-Evaluate the Current IRP

This part needs you to evaluate the current Incident Response Plan (IRP) provided. The plan must be assessed against the following sections from the NIST SP 800-61 Computer Security Incident Handling Guide:

* 2.3.2 – Plan Elements (pg. 8)
* 2.3.3 – Procedure Elements (pg. 8)

Your team will also need to document the potential business impacts of various cyber threats.

The team is to produce a document that makes recommendations to management on how to improve the current incident response plan.

Ensure that the document meets the following requirements:

* Is no longer than two (2) pages
* Is addressed to the Chief Security Officer
* Contains at least five (5) recommendations
* Each recommendation is justified
* Contains the components a CSOC and recommendations to implement a CSOC

# Part 5 Developing the IRP

In this part, the team will develop the IRP. This means that by the end of this part, the Incident Response Team Exercise (IRTx) will be ready to run, including all the necessary resources.

* The following are tasks that are required. However, the team may include other tasks as required:
* The parameters of the IRTx are established:
* Rules of engagement are developed
* Red Team playbook developed
  + Define the range of attacks to be used.
  + Methods of attack outlined / developed
  + Using software such as Kali Linux, Metasploit etc
  + Red team must include pre-prepared PCAP files (if required) in the SIEM
* Blue Team playbook developed
  + Services provided by the IRT are defined (such as Firewalls, IDS/IPS, End Point Protection, Network monitoring, Wireshark, etc)
  + Response handling plan for a range of incidents developed
  + Incident response reporting / communication process developed
  + Evidence collection and protection process developed
* Observer Team checklist developed
  + Evaluate Blue Team performance against processes developed (Note: Class Teacher to be the Observer Team)
* Resource Development
  + All playbooks, checklists, procedures have been developed and are ready for deployment / use
  + Virtual machines are obtained / created, checked, and configured for IRTx requirements
  + Prepared PCAP file installed
  + Manual injects developed and ready for use.
* The following planning cycle must be used (refer to the Cyber Exercise Playbook for descriptions) (Note: The Cyber Exercise Playbook is referenced throughout this task)

# Part 6: Stakeholder Status Report / Teacher Meeting

As for the communications plan, the team will need to give a stakeholder status report and meet with the project sponsor. These meetings can be combined as the project sponsor is also a project stakeholder.

Each week your team is required to provide a written project status report to the project stakeholder. This report must include, but is not limited to:

* Overall project status
* Milestone review – Actual vs Planned
* Issues and risks – What were the issues for the week and what was the risk/impact of these issues on the overall status?
* Timeline – Actual vs Targeted
* Work completed: Which tasks have been successfully completed. A link to a report template is provided below.
* Identify end user training needs

The meeting with your teacher is intended to be an informal meeting to ensure the team is working together and to provide support if required.

# Deliverables

1. Project charter based on the given template
2. Briefing report and meeting minutes to establish the project team
3. Communication plan based on the given template
4. Recommendation to IRP
5. Updated IRP
6. Weekly status reports

# Documentation requirements are as follows:

* Written report format is appropriate
* Document is logically organised
* Written language is appropriate for the communication purpose
* Each team member has signed off on the report
* Reports were submitted on time

**End of Assessment**